II. CLAIM AMENDMENTS

1. (Previously Presented) A method for transmitting data between a radio access network of a packet-switched time division multiple access mobile system and user equipment of a mobile system, comprising the steps of:

encrypting the data to be transmitted using an encryption algorithm at a transmitting end,

transmitting the encrypted data from the transmitting end to a receiving end,

decrypting the transmitted data using an encryption algorithm at the receiving end,

wherein an encryption algorithm of a radio access network of a wideband code division multiple access mobile system is used as the encryption algorithm, in which case input parameters of agreed format required by the encryption algorithm are created on the basis of operating parameters of the radio access network of the packet-switched time division multiple access mobile system.

2. (Original) A method as claimed in claim 1, wherein the agreed format of the input parameters of the encryption algorithm defines the number of the input parameters and the length of each parameter.

3. (Previously Presented) A method as claimed in claim 1, wherein the encryption algorithm is a black box and implementation of the encryption algorithm is exactly the same in both the radio access network of the packet-switched time division multiple access mobile system and the radio access network of the wideband code division multiple access mobile system.

4. (Original) A method as claimed in claim 1, wherein the input parameters comprise a counter parameter.

5. (Previously Presented) A method as claimed in claim 4, wherein the counter parameter comprises a symbol which defines whether the data to be encrypted is data of a second layer signaling plane or other data.

6. (Original) A method as claimed in claim 1, wherein the input parameters comprise a bearer parameter, and one of the bearer parameter values is reserved for signaling plane data to be encrypted.

7. (Previously Presented) A method as claimed in claim 4, wherein when executing the encryption algorithm in a MAC layer of a protocol stack, the counter parameter comprises an extended TDMA frame number.

8. (Previously Presented) A method as claimed in claim 7, wherein the extended TDMA frame number is based on extending a T1 counter part of GSM.

9. (Previously Presented) A method as claimed in claim 7, wherein information on a last used extended TDMA frame number is stored in the user equipment for a next connection.

10. (Original) A method as claimed in claim 9, wherein the information to be stored on the last used extended TDMA frame number comprises a certain number of the most significant bits of the extended TDMA frame number, and before the information is used

in a new radio connection to form an extended TDMA frame number, the value of the number formed by said most significant bits is increased by one.

11. (Previously Presented) A method as claimed in claim 4, wherein when executing the encryption algorithm in a MAC layer of a protocol stack, the counter parameter comprises a time slot number.

12. (Previously Presented) A method as claimed in claim 4, wherein when executing the encryption algorithm in an RLC layer of a protocol stack, the counter parameter comprises a hyper frame number.

13. (Previously Presented) A method as claimed in claim 12, wherein information is stored on a last used hyper frame number in the user equipment for a next connection, and before the information is used in a new radio connection to form a hyper frame number, the value of the number is increased by one.

14. (Previously Presented) A method as claimed in claim 13, wherein the information to be stored on the last used hyper frame number comprises a certain number of most significant bits of the hyper frame number.

15. (Previously Presented) A method as claimed in claim 1, wherein when a connection of the user equipment changes between the radio access network of the packet-switched time division multiple access mobile system and the radio access network of the wideband code division multiple access mobile system, information on a last used extended TDMA frame number or hyper frame number is provided to a new radio access network, and the same encryption key input parameter as in an old radio access network

is used as the encryption key input parameter of the encryption algorithm in the new radio access network.

16. (Original) A method as claimed in claim 15, wherein the information to be provided comprises a certain number of most significant bits, and before the information is used in a new radio access network, the value of the number formed by said most significant bits is increased by one.

17. (Previously Presented) User equipment of a mobile system, comprising

means for encrypting data to be transmitted to a radio access network of a packet-switched time division multiple access mobile system using an encryption algorithm,

means for decrypting data received from the radio access network of the packet-switched time division multiple access mobile system using an encryption algorithm;

wherein the encryption algorithm is an encryption algorithm of a radio access network of a wideband code division multiple access mobile system, and the user equipment comprises means for creating input parameters of agreed format required by the encryption algorithm on the basis of operating parameters of the radio access network of the packet-switched time division multiple access mobile system.

18. (Original) User equipment as claimed in claim 17, wherein the agreed format of the input parameters of the encryption algorithm defines the number of the input parameters and the length of each parameter.

19. (Previously Presented) User equipment as claimed in claim 17, wherein the encryption algorithm is a black box and implementation of the encryption algorithm is exactly the same in both the radio access network of the packet-switched time division multiple access mobile system and the radio access network of the wideband code division multiple access mobile system.

20. (Original) User equipment as claimed in claim 17, wherein the input parameters comprise a counter parameter.

21. (Previously Presented) User equipment as claimed in claim 20, wherein the counter parameter comprises a symbol which defines whether the data to be encrypted is data of a second layer signaling plane or other data.

22. (Original) User equipment as claimed in claim 17, wherein the input parameters comprise a bearer parameter, and one of the bearer parameter values is reserved for signaling plane data to be encrypted.

23. (Previously Presented) User equipment as claimed in claim 20, wherein when executing the encryption algorithm in a MAC layer of a protocol stack, the counter parameter comprises an extended TDMA frame number.

24. (Previously Presented) User equipment as claimed in claim 23, wherein the extended TDMA frame number is based on extending a T1 counter part of GSM.

25. (Previously Presented) User equipment as claimed in claim 23, wherein the user equipment comprises means for storing information on a last used extended TDMA frame number for a next connection.

26. (Original) User equipment as claimed in claim 25, wherein the information to be stored on the last used extended TDMA frame number comprises a certain number of the most significant bits of the extended TDMA frame number, and the user equipment comprises means for increasing by one the value of the number formed by said most significant bits before the information is used in a new radio connection to form an extended TDMA frame number.

27. (Previously Presented) User equipment as claimed in claim 20, wherein when executing the encryption algorithm in a MAC layer of a protocol stack, the counter parameter comprises a time slot number.

28. (Previously Presented) User equipment as claimed in claim 20, wherein when executing the encryption algorithm in an RLC layer of a protocol stack, the counter parameter comprises a hyper frame number.

29. (Previously Presented) User equipment as claimed in claim 28, wherein the user equipment comprises means for storing information on a last used hyper frame number for a next connection.

30. (Original) User equipment as claimed in claim 29, wherein the information to be stored on the last used hyper frame number comprises a certain number of the most significant bits of the hyper frame number, and the user equipment comprises means for

increasing by one the value of the number formed by said most significant bits before the information is used in a new radio connection to form a hyper frame number.

31. (Previously Presented) User equipment as claimed in claim 17, wherein the user equipment comprises means for providing information on a last used extended TDMA frame number or hyper frame number to a new radio access network when a connection of the user equipment changes between the radio access network of a packet-switched time division multiple access mobile system and the radio access network of the wideband code division multiple access mobile system, and for using the same encryption key parameter as in an old radio access network as the encryption key parameter of the encryption algorithm in the new radio access network.

32. (Original) User equipment as claimed in claim 31, wherein the information to be provided comprises a certain number of most significant bits, and the user equipment comprises means for increasing by one the value of the number formed by said most significant bits before the information is used in a new radio access network.

33. (Previously Presented) A radio access network of a packet-switched time division multiple access mobile system of a mobile system, comprising

means for encrypting data to be transmitted to user equipment using an encryption algorithm,

means for decrypting data received from the user equipment using the encryption algorithm;

wherein the encryption algorithm is an encryption algorithm of a radio access network of a wideband code division multiple access mobile system, and the radio

access network of the packet-switched time division multiple access mobile system comprises means for creating input parameters of agreed format required by the encryption algorithm on the basis of operating parameters of the radio access network of the packet-switched time division multiple access mobile system.

34. (Original) A radio access network as claimed in claim 33, wherein the agreed format of the input parameters of the encryption algorithm defines the number of the input parameters and the length of each parameter.

35. (Previously Presented) A radio access network as claimed in claim 33, wherein the encryption algorithm is a black box and implementation of the encryption algorithm is exactly the same in both the radio access network of the packet-switched time division multiple access mobile system and the radio access network of the wideband code division multiple access mobile system.

36. (Previously Presented) A radio access network as claimed in claim 33, wherein the input parameters comprise a counter parameter.

37. (Previously Presented) A radio access network as claimed in claim 36, wherein the counter parameter comprises a symbol which defines whether the data to be encrypted is data of a second layer signaling plane or other data.

38. (Previously Presented) A radio access network as claimed in claim 37, wherein the input parameters comprise a bearer parameter, and one of the bearer parameter values is reserved for signaling plane data to be encrypted.

39. (Previously Presented) A radio access network as claimed in claim 36, wherein when executing the encryption algorithm in a MAC layer of a protocol stack, the counter parameter comprises an extended TDMA frame number.

40. (Previously Presented) A radio access network as claimed in claim 39, wherein the extended TDMA frame number is based on extending a T1 counter part of GSM.

41. (Previously Presented) A radio access network as claimed in claim 39, wherein the radio access network of the packet-switched time division multiple access mobile system comprises means for storing information on a last used extended TDMA frame number for a next connection.

42. (Previously Presented) A radio access network as claimed in claim 41, wherein the information to be stored on the last used extended TDMA frame number comprises a certain number of the most significant bits of the extended TDMA frame number, and the radio access network of the packet-switched time division multiple access mobile system comprises means for increasing by one the value of the number formed by said most significant bits before the information is used to form an extended TDMA frame number.

43. (Previously Presented) A radio access network as claimed in claim 36, wherein when executing the encryption algorithm in a MAC layer of a protocol stack, the counter parameter comprises a time slot number.

44. (Previously Presented) A radio access network as claimed in claim 36, wherein when executing the encryption algorithm in an RLC layer of a protocol stack, the counter parameter comprises a hyper frame number.

45. (Previously Presented) A radio access network as claimed in claim 44, wherein the radio access network of the packet-switched time division multiple access mobile system comprises means for storing information on a last used hyper frame number for a next connection.

46. (Previously Presented) A radio access network as claimed in claim 45, wherein the information to be stored on the last used hyper frame number comprises a certain number of the most significant bits of the hyper frame number, and the radio access network of the packet-switched time division multiple access mobile system comprises means for increasing by one the value of the number formed by said most significant bits before the information is used to form a hyper frame number.

47. (Previously Presented) A radio access network as claimed in claim 33, wherein the radio access network of the packet-switched time division multiple access mobile system comprises means for receiving information on a last used extended TDMA frame number or hyper frame number to the user equipment when a connection of the user equipment changes between the radio access network of the packet-switched time division multiple access mobile system and the radio access network wideband code division multiple access mobile system, and for using as the encryption key parameter of the encryption algorithm, the encryption key parameter according to the received information.

48. (Previously Presented) A radio access network as claimed in claim 47, wherein the information to be provided comprises a certain number of most significant bits, and the

radio access network of the packet-switched time division multiple access mobile system comprises means for increasing by one the value of the number formed by said most significant bits before the information is used.